Michigan Telecommunications and Technology Law Review

Volume 8 | Issue 1

2002

Marking Carnivore's Territory: Rethinking Pen Registers on the Internet

Anthony E. Orr
University of Michigan Law School

Follow this and additional works at: http://repository.law.umich.edu/mttlr

 Part of the Fourth Amendment Commons, Internet Law Commons, National Security Law Commons, and the Privacy Law Commons

Recommended Citation

Anthony E. Orr, *Marking Carnivore's Territory: Rethinking Pen Registers on the Internet*, 8 Mich. Telecomm. & Tech. L. Rev. 219 (2002).
Available at: http://repository.law.umich.edu/mttlr/vol8/iss1/5

This Note is brought to you for free and open access by the Journals at University of Michigan Law School Scholarship Repository. It has been accepted for inclusion in Michigan Telecommunications and Technology Law Review by an authorized editor of University of Michigan Law School Scholarship Repository. For more information, please contact mlaw.repository@umich.edu.

NOTE

MARKING CARNIVORE'S TERRITORY: RETHINKING PEN REGISTERS ON THE INTERNET

*Anthony E. Orr**

Cite as: Anthony E. Orr, *Marking Carnivore's Territory: Rethinking Pen Registers on the Internet*, 8 MICH. TELECOMM. TECH. L. REV. 219 (2002), *available at* http://www.mttlr.org/voleight/orr.pdf

* Indiana University, B.A. 1998; University of Michigan Law School, J.D. candidate 2002. Mr. Orr is an Executive Article Editor of the Michigan Telecommunications and Technology Law Review and a Contributing Editor of the Michigan Journal of International Law.

PART I. INTRODUCTION

"Carnivore" entered the online world's collective consciousness in June 2000 when the Federal Bureau of Investigation unveiled the Internet surveillance software program to telecommunications industry specialists.[1] The FBI claims the program allows agents to scan the traffic of an Internet Service Provider (ISP) for messages or commands to or from a criminal suspect and then intercept only those messages, capturing copies of e-mails, web site downloads and other file transfers.[2]

Reactions to Carnivore were immediate and frequently as vicious as the program's moniker. Privacy advocates warned that the program posed serious threats to the online privacy of law-abiding citizens, as it created the potential for widespread monitoring of Internet traffic.[3] Internet Service Providers balked at the notion of an outside entity installing a device, over which they would have no control, on their networks.[4] An oversight panel of the House Judiciary Committee convened a hearing on Carnivore on July 24, 2000, during which committee members demanded that FBI officials prove that the software captures only those messages pertaining to a criminal suspect and no others.[5] The Senate Judiciary Committee followed suit on September 6, 2000. Throughout the debate, FBI officials have steadfastly maintained that deployment of the program is sufficiently restricted by current law and internal reviews to prevent misuse.[6]

A central issue in the controversy surrounding Carnivore is whether current law permits the FBI to employ the program in the Internet context. Bureau officials claim statutory authority for deployments under

1. Neil King Jr. & Ted Bridis, *FBI's Wiretaps to Scan E-Mail Spark Concern*, WALL ST. J., July 11, 2000, at A3.

2. Ted Bridis & Neil King Jr., *Carnivore E-Mail Tool Won't Eat Up Privacy, Says FBI*, WALL ST. J., July 20, 2000, at A28.

3. *See* King Jr. and Bridis, *supra* note 1, at A3.

4. Nick Wingfield & Don Clark, *Internet Companies Decry FBI's E-Mail Wiretap Plan*, WALL ST. J., July 12, 2000, at B11A.

5. Ted Bridis, *Congressional Panel Debates Carnivore As FBI Moves to Mollify Privacy Worries*, WALL ST. J., July 25, 2000, at A24.

6. *Id.*

three provisions originally enacted to regulate telephone surveillance—Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III)[7] and the Electronic Communications Privacy Act of 1986 (ECPA)[8]—and a statute governing retrieval of "transactional records" of communications—the Communication Assistance for Law Enforcement Act of 1994 (CALEA)[9].[10] Title III governs the use of electronic surveillance to capture the full content of communications, commonly referred to as "wiretapping."[11] The ECPA is concerned with the use of "pen register" devices—which traditionally allowed law enforcement officers to record the telephone numbers dialed from a suspect's telephone[12]—and "trap and trace" devices—which traditionally involved capturing the originating telephone numbers of incoming calls to a criminal suspect, like caller ID devices.[13] In a manner not entirely clear, FBI officials justify interception of e-mail addressing information under a conflation of ECPA and CALEA.[14]

The FBI cites *Smith v. Maryland*[15] for constitutional authority to employ the pen register and trap and trace functions of Carnivore. *Smith* holds that telephone customers have no reasonable expectation of privacy in the electronic impulses dialed and transmitted over telephone lines to initiate a telephone call.[16] By analogy, Bureau officials assert that they are entitled to obtain a court order to install Carnivore as a pen register or trap and trace capable of intercepting the Internet Protocol (IP) addresses and "To:" and "From:" fields of e-mails coming to or originating from a criminal suspect.[17]

While the pen register and trap and trace functions are neither the most controversial nor potentially invasive aspects of Carnivore, they are at least the most legally contestable of its uses. The FBI's assertion of constitutional and statutory authority to employ these functions on the Internet are challenged by those who believe a pen register capturing IP address and/or header information from e-mail messages falls outside

7. 18 U.S.C. §§ 2510–2522 (1994).
8. 18 U.S.C. §§ 3121–3127 (1994).
9. 18 U.S.C. § 2703 (Supp. II 1996).
10. *The 'Carnivore' Controversy: Electronic Surveillance and Privacy in the Digital Age: Hearing Before the Senate Comm. on the Judiciary*, 106th Cong. (2000) [hereinafter "Senate Hearing"] (statement of Donald M. Kerr, Assistant Director, Federal Bureau of Investigation), *available at* http://www.senate.gov/~judiciary/962000_dmk.htm (last visited Nov. 19, 2001).
11. 18 U.S.C. § 2516 (1994).
12. 18 U.S.C. § 3127(3) (1994).
13. 18 U.S.C. § 3127(4) (1994).
14. *Senate Hearing*, *supra* note 10 (statement of Donald M. Kerr).
15. 442 U.S. 735 (1979).
16. *Id.*
17. *Id.*

the scope contemplated by the courts and Congress for pen registers.[18] This note explores this question, drawing on statutes and case law that form the foundation of authority for electronic surveillance.

Part II provides a brief overview of the Carnivore system and its capabilities. Part III elaborates on the statutory and constitutional authority for pen register and trap and trace devices[19] in the traditional telephone context, as well as the legal requirements for obtaining a court order to install such a device. Part IV analyzes the FBI's proposed justification for Internet use and concludes that while constitutional authority exists for pen register applications of Carnivore, statutory authority derives from sections imposing higher evidentiary standards on law enforcement than the pen register statutes. Part V recommends that Internet pen register orders be issued only upon satisfaction of the stricter evidentiary standard of 18 U.S.C. § 2703.

PART II. CARNIVORE AND ITS CAPABILITIES

Under pressure from both legislators and privacy advocates, the FBI submitted Carnivore to independent expert review[20] at the Illinois Institute of Technology Research Institute (IITRI) and the Illinois Institute of Technology Chicago-Kent School of Law. In response, the group issued a draft report in November 2000, providing a complete description of the Carnivore system's capabilities and limitations.[21]

The Carnivore software program is installed on a general purpose desktop computer, which is connected, without keyboard or monitor, to a switch or hub at an ISP.[22] The computer receives all of the data "packets" passing through the segment of the ISP's network to which it is attached.[23] The "collection computer," as this unit is called, is remotely controlled by an FBI computer connected via telephone link by the

18. *Senate Hearing*, *supra* note 10 (statement of Senator Patrick Leahy), *available at* http://www.senate.gov/~judiciary/96200_pjl.htm.

19. Though differing slightly in function and statutory wording, the legal principles discussed apply in the same manner to both pen registers and trap and trace devices, which will be referred to collectively as pen registers.

20. Bridis, *supra* note 5, at A24.

21. ILLINOIS INSTITUTE OF TECHNOLOGY RESEARCH INSTITUTE, INDEPENDENT TECHNICAL REVIEW OF THE CARNIVORE SYSTEM: DRAFT REPORT, Nov. 17, 2000, *available at* http://www.usdoj.gov/jmd/publications/carnivore_draft_1.pdf.

22. *Id.* at vii–ix.

23. *Id.*

commercially available PCAnywhere® software.[24] All computers are equipped with a Jaz® drive for removable data storage.[25]

The defining feature of Carnivore is its ability to "filter" a single suspect's Internet traffic from among that of all users on a portion of the ISP's network, and then capture (by making a copy of the data packets) only those types of data authorized by court order.[26] Using a relatively simple Windows®-based interface, an FBI agent may set Carnivore to capture data packets originating from or destined for a particular e-mail or IP addresses, whether fixed or dynamically assigned.[27] In wiretap mode, the system can view the content of e-mails, Hypertext Transfer Protocol (HTTP, or World Wide Web) pages, File Transfer Protocol (FTP) sessions, or any other application protocols.[28] In pen register mode, the program can collect header information such as the "To:" and "From:" addresses from e-mails and the IP addresses of computers involved in FTP or HTTP transactions.[29]

Captured data packets are archived for analysis. A software program called Packeteer® processes the raw output of Carnivore to reconstruct the higher-level protocols (e.g., HTTP) from the data packets, each of which represents only a small portion of any given message.[30] The reconstructed data is then analyzed by a program called CoolMiner®, which develops statistical summaries and displays pen register or full content information via an Internet browser.[31]

The IITRI report concluded that when used correctly pursuant to a Title III wiretap order, Carnivore provides law enforcement officials with no more information than is permitted by the court order.[32] This success depends, however, on the ability of the operating agent to properly configure the filters.[33] Even when correctly configured in pen register mode, the IITRI report found that Carnivore collects "To:" and "From:" fields from e-mail, as well as the length of messages and the length of individual fields within those messages, possibly exceeding the scope of the authorizing court order.[34]

---

24. *Id.*
25. *Id.*
26. Federal Bureau of Investigation, *Carnivore Diagnostic Tool, at* http://www.fbi.gov/hq/lab/carnivore/carnivore2.htm (last visited Nov. 19, 2001).
27. ILLINOIS INSTITUTE OF TECHNOLOGY RESEARCH INSTITUTE, *supra* note 21, at ix–x.
28. *Id.* at ix.
29. *Id.*
30. *Id.* at xii.
31. *Id.*
32. *Id.* at xii.
33. *Id.* at xi.
34. *Id.* at xii.

It is worth noting that Carnivore must scan *every* data packet traveling the subnetwork it is monitoring in order to determine which to capture and which to ignore. Those that pertain to the subject of investigation are captured for additional filtering and storage, while the rest are ignored.[35] The IITRI report notes that while Carnivore is designed for "fine-tuned searches," it is also capable of "broad sweeps."[36]

PART III. LEGAL AUTHORITY AND REQUIREMENTS FOR TRADITIONAL PEN REGISTER AND TRAP AND TRACE INSTALLATIONS

Federal law defines a pen register as "a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached."[37] A "trap and trace device" means "a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted."[38]

Law enforcement officials need not obtain a search warrant before installing a pen register or trap and trace device. Federal law requires, however, that an attorney for the government or a law enforcement officer apply for a court order under 18 U.S.C. § 3123 (1994) before employing such a device.[39] This application must include 1) the identity of the attorney or officer making the application and the identity of the law enforcement agency conducting the investigation, and 2) a certification by the applicant (i.e. the applicant's assertion) that the information likely to be obtained from the pen register or trap and trace is "relevant to an ongoing criminal investigation being conducted by that agency."[40] When a proper application is submitted, the magistrate *must* issue an order authorizing the installation and use of a pen register or trap and trace device.[41] The order must specify 1) the identity, if known, of the person to whose telephone line the device will be attached; 2) the identity, if known, of the person who is the subject of the investigation; 3) the telephone number and physical location of the telephone line and, in the

35. *Senate Hearing*, *supra* note 10 (statement of Donald M. Kerr).

36. ILLINOIS INSTITUTE OF TECHNOLOGY RESEARCH INSTITUTE, *supra* note 21, at 4-3; "Incorrectly configured, Carnivore can record any traffic it monitors." *Id.*

37. 18 U.S.C. § 3127(3) (1994).

38. 18 U.S.C. § 3127(4) (1994).

39. 18 U.S.C. §§ 3121(a), 3122(a) (1994).

40. 18 U.S.C. § 3122(b)(1)–(2) (1994).

41. 18 U.S.C. § 3123(a) (1994) ("Upon an application made under section 3122 of this title, the court *shall* enter an ex parte order authorizing the installation and use of a pen register or a trap and trace device within the jurisdiction of the court . . . ." [emphasis added]).

case of a trap and trace, the geographic limits of the order, and 4) a statement of the offense to which the information likely to be obtained relates.[42]

The statutory threshold for obtaining a pen register or trap and trace order is low and easily met; however, even this standard is more than the Constitution requires. In *Smith v. Maryland*, the Supreme Court held that pen registers do not constitute a "search" for Fourth Amendment purposes, and thus require no search warrant or court authorization of any type.[43] The Court reasoned that telephone subscribers have no reasonable expectation of privacy in the numbers they dial; thus, those numbers fall outside the Fourth Amendment's zone of protection.[44] Applying the two-prong expectation of privacy test established in *Katz v. United States*,[45] the *Smith* Court held that a telephone subscriber cannot have a subjective expectation of privacy in numbers dialed, for all telephone customers know that the numbers they dial are revealed to and recorded by the phone company in the normal course of business, both for connecting their calls and for other purposes.[46] Furthermore, even if a customer oblivious to these facts entertained a subjective expectation of privacy, the Court held that this expectation was not one society recognizes as objectively reasonable.[47] This result follows, the Court said, from the doctrine that a person has no legitimate expectation of privacy in information he voluntarily turns over to a third party (i.e. the telephone company).[48] Thus, when a telephone subscriber "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business," the subscriber "assumed the risk that the company would reveal to police the numbers he dialed."[49]

---

42. 10 U.S.C. § 3123(b)(1)(A)–(D) (1994).

43. Smith v. Maryland, 442 U.S. 735, 745–46, (1979).

44. *See id.*

45. 389 U.S. 347, (1967). To determine whether the Fourth Amendment applies to a communication, the *Katz* test asks two questions: 1) whether, by his conduct, the individual "exhibited an actual (subjective) expectation of privacy" in the communication, and 2) whether the individual's subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable.'" *Katz*, 389 U.S. at 361.

46. *Smith*, 442 U.S. at 742–43.

47. *Id.* at 743.

48. *Id.* at 743–44.

49. *Id.* at 744.

PART IV. CURRENT LAW DOES NOT AUTHORIZE USE OF CARNIVORE AS AN "INTERNET PEN REGISTER" TO CAPTURE E-MAIL ADDRESSING INFORMATION UNDER 18 U.S.C. § 3123

The aforementioned statutes and constitutional principles are now routinely applied to pen registers and trap and trace devices installed on telephone lines. Over the last three years, the FBI and numerous courts have applied them to Carnivore installations as well, authorizing the use of the program as an "Internet pen register" to capture the "To:" and "From:" fields on e-mail messages. While the FBI views telephone and Internet pen registers as clearly analogous, and subject to the same laws,[50] others argue that the Bureau lacks legal authority to capture e-mail addressing information in particular, because it is more revealing than the numbers dialed on a telephone.[51] Viewed from the standpoint of how each type of information is used, Carnivore likely meets the constitutional requirements for implementation of a pen register. Neither the literal statutory language nor statutory construction, however, support the application of ECPA to a pen register in the Internet context.

A. *Carnivore Meets Constitutional Requirements for Pen Registers*

1. Carnivore Under Smith v. Maryland

The language of *Smith v. Maryland* makes it difficult to conclude definitively whether Internet users hold any reasonable expectation of privacy in e-mail addressing information. If they do, a Carnivore pen register order constitutes a "search" for Fourth Amendment purposes and law enforcement officials would be required to show probable cause to obtain such an order.[52] If no reasonable expectation exists, and e-mail addressing information is analogous to telephone numbers, the FBI's use of Internet pen registers without a showing of probable cause is proper, from a constitutional law standpoint.[53]

a. Users Have No Subjective Expectation of Privacy in E-mail Addressing Information

The primary difficulty in drawing the necessary analogy lies in the *Smith* Court's exclusive focus on telephone pen registers. The Court's

50. *Senate Hearing*, *supra* note 10 (statement of Donald M. Kerr).

51. *Id.* (statement of Gregory T. Nojeim, Legislative Counsel, American Civil Liberties Union), *available at* http://www.aclu.org/congress/1040600a.html (last visited Nov. 19, 2001).

52. U.S. CONST. amend. IV.

53. *Smith*, 442 U.S. at 745–46.

rationale for determining that telephone subscribers hold no subjective expectation of privacy in the numbers they dial draws much of its strength from the billing structure of the telephone industry. The Court argued that because telephone subscribers know that the numbers they dial are recorded by the telephone company for billing toll calls (i.e., their monthly bills list the numbers they called) and for applying special rate structures, they also know that the telephone company can record the numbers they dial.[54] Buttressing this argument are other characteristics of how telephone systems use telephone numbers—subscribers realize they must "convey" phone numbers to the telephone company for purposes of completing their calls; devices recording telephone numbers are frequently used to check billing operations, detect fraud and prevent violations of the law; pen registers are used to determine whether a customer is using a home phone to conduct a business; and recorded telephone records are used to identify persons making annoying or obscene calls.[55] The Court concluded,

> Telephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes.... [I]t is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.[56]

The wording of this summary provides the strongest support for denying that Internet users hold a subjective expectation of privacy in e-mail addressing information. On the one hand, the billing structure of ISPs, typically consisting of a flat monthly fee or a fee based on time spent online, never considers the distance over which messages are sent. Consequently, the recipient addresses of such messages play no part in determining billing, and no itemized list of "numbers dialed" is received by users to destroy an expectation of privacy. But when users send e-mail messages, they certainly know that addressing information is being "conveyed" to their ISP, if for no other reason than to route their messages to the proper destination. Moreover, because e-mail is typically stored on an ISP's server computer before it is read by a recipient, and often remains there after reading, users know ISPs possess "facilities for recording" e-mail addressing information. The recordability of e-mail

54. *Id.* at 742.
55. *See id.*
56. *Id.* at 743.

addresses is further supported by the knowledge that e-mail, like all Internet traffic, is composed of digital data that may easily be recorded by any computer receiving it. And for many of the reasons articulated by the *Smith* Court—particularly detecting fraud and identifying the source of harassing or obscene messages—users likely expect their ISPs to occasionally or regularly record the addressing information of certain messages for "legitimate business purposes." Considering these auxiliary functions of e-mail addressing, it is "too much to believe"[57] that Internet users expect their addressing information to remain private.

b. Society Does Not Recognize an Objective Expectation of Privacy in E-mail Addressing Information

Supposing *arguendo*, however, that an Internet user could somehow manifest a subjective expectation of privacy in her e-mail addressing information, the second prong of the *Katz* test remains to be satisfied—is that expectation one that society is willing to recognize as objectively reasonable?[58] Omitting any discussion of competing social policies or societal norms, the *Smith* Court answered this question in the negative in the telephone context,[59] based on the "assumption of risk" doctrine of *United States v. Miller*.[60] The *Smith* Court interpreted *Miller* to stand for the proposition that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[61] The *Miller* Court held that a bank depositor has no "legitimate 'expectation of privacy' " in financial information "voluntarily conveyed to . . . banks and exposed to their employees in the ordinary course of business."[62] Thus, explained the *Miller* Court,

> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. . . . [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[63]

57. *Smith*, 442 U.S. at 743.
58. *See Katz*, 389 U.S. at 361.
59. *Smith*, 442 U.S. at 743–44.
60. 425 U.S. 435 (1976).
61. *Smith*, 442 U.S. at 743–44 (citing *Miller*, 425 U.S. at 442–44).
62. *Smith*, 442 U.S. at 744 (quoting *Miller*, 425 U.S. at 442).
63. *Id.* (quoting *Miller*, 425 U.S. at 443).

With no discussion of the difference between financial records and telephone numbers, the *Smith* Court analogized,

> When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and "exposed" that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed. The switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls to the subscriber.[64]

Substituting the proper e-mail terms into this formula, it becomes clear that e-mail addressing information revealed to no one other than an ISP's equipment nevertheless falls squarely within the *Miller* assumption of risk doctrine, as interpreted in *Smith*. Telephone numbers dialed and e-mail addressing information serve the same legitimate business purpose—both tell network switching equipment where to send the call or message of the initiating party. The fact that no human being may ever view the header information is of no consequence. When an Internet user sends a message over an ISP's network, she has revealed the addressing information to the ISP's equipment in the ordinary course of business, and she assumes the risk that the ISP will reveal her addressing information to the government. A Carnivore installation on the ISP network simply facilitates this "revelation" by the ISP.[65]

2. Carnivore's Constitutional Challenges

Having established doctrinally that Internet users have neither a subjective nor an objective expectation of privacy in e-mail addressing information per *Smith*, one additional wrinkle casts some doubt on whether Carnivore pen register installations are constitutional. The *Smith* Court emphasized very clearly the importance that the limited functionality of a telephone pen register played in its opinion:

> Indeed, a law enforcement official could not even determine from the use of a pen register whether a communication existed. . . . They disclose only the telephone numbers that have been dialed—a means of establishing communication. Neither the purport of any communication between the caller and the

64. *Smith*, 442 U.S. at 744.

65. Note that the revelation by the third party to the Government need not be voluntary. The bank records disclosed in *Miller* were obtained by means of subpoenas duces tecum. *Miller*, 425 U.S. at 436.

> recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers.[66]

Two aspects of the Carnivore system raise concerns in light of this qualification. First, recall that the IITRI Draft Report on Carnivore found that the system collects more than simply addressing information from e-mail. The report noted that when correctly configured in pen register mode, Carnivore collects not only the "To:" and "From:" fields of targeted e-mail messages, but also the length of the message and the length of individual fields within those messages.[67] In fact, the system captures the entire e-mail message and all of its fields (including the "SUBJECT" line and contents of the message), but replaces each character in fields other than "To:" and "From:" with an X.[68]

Certainly this information reveals more than the analog to "numbers dialed." While not revealing to law enforcement the subject of the message, whether the message contains any illegal content, etc., it does indicate "whether a communication existed" or "whether the call was even completed."[69] Considering the *Smith* Court's solicitude over the limited nature of pen registers, this fact raises the question whether Carnivore, in its current incarnation, fully meets the constitutional definition of a pen register, or moves closer to the content-collecting realm of a full Title III wiretap.

The second potential constitutional problem with Carnivore is contained in suggestions by some that e-mail addressing information itself is more revealing of identity than mere telephone numbers.[70] An e-mail address typically consists of a username connected to a server name by "@" (e.g., student@umich.edu). The username is typically assigned to one individual for institutional e-mail accounts (e.g., university and business), but may be used by multiple members of a single household in the case of a private ISP account. In the institutional settings mentioned, usernames are often assigned by a central authority and typically contain some part of the user's proper name. Private ISPs typically permit customers to choose their own usernames, within certain parameters. Very frequently these usernames also contain variations on or parts of the customer's proper name. Some ISPs allow individuals within a household

---

66. *Smith*, 442 U.S. at 741 (quoting United States v. New York Tel. Co., 434 U.S. 159, 167 (1977)).

67. ILLINOIS INSTITUTE OF TECHNOLOGY RESEARCH INSTITUTE, *supra* note 21, at xii.

68. *Id.* at 4-3.

69. *Smith*, 442 U.S. at 741 (quoting United States v. New York Tel. Co., 434 U.S. 159, 167 (1977)).

70. *Senate Hearing*, *supra* note 10 (statement of Senator Patrick Leahy).

using the same Internet access account to create their own unique usernames.

With these characteristics in mind, it appears e-mail addressing information often does reveal more about the identity of the sender and receiver than the ten simple digits of a telephone number. But one may well question whether this fact is necessarily troublesome from a constitutional standpoint. It is unclear whether an e-mail address more accurately reveals the *actual* sender or recipient of an e-mail than does a telephone number. For someone other than the owner named in the records of the telephone company or ISP to use either type of account, access must be gained. For an e-mail account, this means the user must be privy to the owner's password. However, e-mail accounts can typically be accessed from almost any geographic location. For a telephone call, the user must gain access to the owner's actual home, where the telephone line terminates. In either case, such access is most likely to be had by other members of the owner's household. Indeed, access to both telephones and e-mail accounts by multiple members of the same household is quite common. Thus, it is unclear whether e-mail addresses really reveal that much more about the identity of message senders and recipients. With no particular guidance from the *Smith* Court as to how important this factor is to its analysis, drawing conclusions about the constitutional importance of the supposed revealing nature of e-mail addressing information would be an exercise in speculation.[71]

Whether e-mail addresses themselves reveal too much information, and thus any pen register use of Carnivore is a violation of the Fourth Amendment, is a policy question that will eventually require judicial or legislative resolution. But it need not presently hinder the FBI's use of the program. The problem of overcollection identified by the IITRI report, however, may be a fatal constitutional flaw. From the standpoint of information functionality, Carnivore appears to collect more information than constitutionally authorized for a pen register. Unlike telephone numbers and e-mail addressing information, the length of messages and the length of individual fields within those messages is not regularly collected for any legitimate business purpose. This is especially true in the e-mail context—while a telephone company may legitimately record the length of messages for billing purposes, an ISP has no reason to monitor

71. In the institutional settings of universities and business, e-mail accounts are typically assigned to and used exclusively by one individual. E-mail addresses attached to these accounts may, in many cases, accurately reveal the sender or recipient of a message, creating a stronger argument for placing interceptions of messages originating from or destined for an institutional e-mail server outside the scope of *Smith*.

the length of e-mail messages.[72] Particularly troublesome is Carnivore's collection of the entire body of the message in "X" form. This surely raises concerns that if the software can electronically "redact" a message, perhaps it could also un-redact it, revealing the full contents. Short of such an overt violation, the possibility exists that a glitch in the system would prevent the redaction from occurring, with the same result. In either case, the Carnivore system is collecting more than is constitutionally authorized by *Smith*, whether that information is then submitted to electronic minimization or not. In light of the *Smith* Court's insistence that pen registers may only collect the telephone numbers dialed, the version of Carnivore reviewed by the IITRI team appears constitutionally unsound, and should not be authorized for use as an Internet pen register.

To bring Carnivore into compliance with the Fourth Amendment, the FBI must alter the program to eliminate the overcollection of data in pen register mode. The IITRI report not only suggests that this is possible, but provides two suggestions for how it might be accomplished.[73] First, the IITRI team recommended the FBI create two separate versions of Carnivore—one for pen registers and one for full-content collection.[74] Separation of the functions would serve two purposes; not only would it allow the customization of the software to prevent overcollection, but it would also eliminate the risk that the program would be accidentally configured for full-content collection when only a pen register was authorized.[75] Second, the IITRI report provides suggestions for simple software modifications that would prevent Carnivore from overcollecting in pen register mode.[76] The report goes so far as to name the specific instructions that should be captured for Simple Mail Transfer Protocol (SMTP) and Post Office Protocol (POP) e-mail systems.[77] If these alterations are made to the Carnivore software program, it will satisfy the constitutional requirements elaborated in *Smith.*

72. The "length" of messages, by which is meant the length of various fields within a message, including the content field, should be distinguished from the size of an e-mail file, which ISP's do legitimately record to monitor individual usage of server space.

73. ILLINOIS INSTITUTE OF TECHNOLOGY RESEARCH INSTITUTE, *supra* note 21, at A-1.

74. *Id.*

75. *Id.* (noting that the side-by-side placement of the pen mode and full content mode "buttons" on the Carnivore configuration screen creates a risk of accidental misconfigurations).

76. *Id.*

77. *Id.* at A-3.

B. *Carnivore Pen Register Installations Are Not Authorized Under 18 U.S.C. § 3123*

Doctrinally, a slightly modified Carnivore program would meet the constitutional requirements of a pen register device. The Constitution is, however, only the first hurdle law enforcement officers must cross before a pen register installation is legally permissible. The applicability of federal statutes governing pen registers is far more questionable, as the literal statutory language, congressional intent, and judicial decisions concerning other communications technologies suggest the FBI's use of Internet pen registers is not authorized by the ECPA, and thus should not be available under the minimal evidentiary standard applicable to pen register applications.

1. Carnivore Is Incompatible with the Literal Language of and Judicial Interpretation of 18 U.S.C. § 3123

The ECPA defined a pen register as a "device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached."[78] Carnivore, on the other hand, is attached to a hub or switch of an ISP and monitors a portion of the ISP's overall traffic.[79] In pen register mode, it intercepts not "numbers dialed," but e-mail addressing information.[80] The dissonance between the statute's literal language and the physical structure of Carnivore installations was noted in testimony before Congress and raised as an objection to the use of Carnivore as a pen register or trap and trace device.[81]

The reality of a Carnivore installation does not coincide with the plain textual definition of a pen register. Judicial interpretation of the governing statutes in reference to two other technologies support this conclusion. The United States Court of Appeals for the Fourth Circuit held in *Brown v. Waddell*[82] that a digital display pager "clone," used by law enforcement officers to intercept pages sent to a suspected drug dealer, does not fall within the statutory definition of a pen register "in the critical sense that it is not attached to a telephone line." A few weeks later, the United States District Court for the Central District of California reached a similar result in *In re Application of the U.S.A. for an*

78. 18 U.S.C. § 3127(3) (1994).

79. ILLINOIS INSTITUTE OF TECHNOLOGY RESEARCH INSTITUTE, *supra* note 21, at vii–ix.

80. *Id.*

81. *Fourth Amendment Issues Raised by the FBI's 'Carnivore' Program: Oversight Hearing Before the Subcomm. on the Constitution of the House Comm. on the Judiciary*, 106th Cong. (2000) (statement of Robert Corn-Revere, Hogan & Hartson LLP), *available at* http://www.house.gov/judiciary/corn0724.htm (last visited Nov. 21, 2001).

82. 50 F.3d 285, 290–291 (4th Cir. 1995).

Order Authorizing the Use of a Cellular Telephone Digital Analyzer.[83] There the court found that use of a cellular telephone digital analyzer—a device capable of intercepting the electronic serial number (ESN) and telephone number of a particular cellular telephone, as well as the numbers dialed on that phone—was not governed by the ECPA's pen register provisions because it was not attached to a telephone line.[84]

2. Legislative Intent Indicates that Carnivore is Not Authorized by § 3123

Beyond the literal language of 18 USC § 3127 and judicial interpretation thereof, legislative intent also falls squarely on the side of limiting pen registers exclusively to devices attached to telephone lines. In the Glossary section of its report on ECPA, the Senate Judiciary Committee defined both pen registers and trap and trace devices exclusively in relation to telephone applications: "Pen registers are devices that record the telephone numbers to which calls have been placed from a particular telephone. . . . [T]rap and trace devices . . . record the numbers of telephones from which calls have been placed to a particular telephone."[85] The court in *In re Cellular Telephone Digital Analyzer* further noted that in other statutory provisions relating to telephone communications, Congress encompassed "any types [sic] of wire, oral, or electronic communications—regardless of whether the intercepting device was 'attached' to a telephone line. *See, e.g.*, 18 U.S.C. § 2511."[86] Thus, the court concluded, the application of the ECPA's pen register provisions exclusively to devices attached to telephone lines "cannot be assumed to be inadvertent."[87] Likewise, the *Brown* court emphasized that the aforementioned Glossary not only distinguishes between different types of pagers, showing that Congress was well aware of the distinctive characteristics of specific technologies, but also defines pen registers separately, indicating a belief that they were distinct and merited technology-specific treatment.[88] The totality of this evidence strongly suggests that Congress envisaged pen registers solely in the telephone context, and so limited the scope of the pen register statutes by its choice of definitive and statutory language.

---

83. 885 F. Supp. 197 (C.D. Cal. 1995).

84. *In re Cellular Telephone Digital Analyzer*, 885 F. Supp. at 200.

85. S. RPT. No. 99-541, pt. 4, at 10 (1986), *reprinted in* 1986 U.S.S.C.A.N. 3555, 3564.

86. *In re Cellular Telephone Digital Analyzer*, 885 F. Supp. at 200.

87. *Id.*

88. *Brown v. Waddell*, 50 F.3d 285, 292 (4th Cir. 1995); *see* S. REP. No. 99-541, *supra* note 85, at 9–10, *reprinted in* 1986 U.S.S.C.A.N. at 3563–3564.

3. The Communications Assistance for Law Enforcement Act Explicitly Imposes a Higher Standard of Proof for Intercepting E-mail Addressing Information

That Congress did not intend to extend the use of pen registers (and the accompanying low standard of proof) to the e-mail context is perhaps evidenced most clearly by its passage of another act—the 1994 Communications Assistance for Law Enforcement Act (CALEA). Section 207 of CALEA instituted two related changes that heightened protection of e-mail addressing information. First, it amended statutes governing access to transactional records to eliminate the ability of law enforcement officials to obtain, by serving a subpoena on an electronic communications services provider, the "addresses on [a subscriber's] electronic messages."[89] Section 207 then proceeded to create an "intermediate standard" that law enforcement must meet before a court will issue an order authorizing the acquisition of such addressing information.[90]

The requirements for government access to "transactional records" relating to electronic communications service (which includes e-mail addressing information) are set forth in 18 U.S.C. § 2703. CALEA section 207(a) amended 18 U.S.C. § 2703(c)(1)(B) by striking a clause that previously allowed law enforcement officers to obtain records concerning a subscriber's electronic communication service by serving a subpoena on the service provider. The House Judiciary Committee acknowledged that the change was motivated by its determination that "transactional records from on-line communication systems reveal much more than telephone toll records or mail covers."[91] Accordingly, the revised statute allows law enforcement officers to access e-mail addressing information by only three means: 1) a full search warrant based upon probable cause, 2) consent of the subscriber or customer whose information will be disclosed, or 3) a court order pursuant to 18 U.S.C. § 2703(d).[92]

Section 207's second innovation was the creation of the "intermediate standard" for obtaining a § 2703(d) court order.[93] Falling somewhere between a subpoena and probable cause, the standard requires that such an order "shall issue only if the governmental entity offers *specific and articulable facts* showing that there are *reasonable grounds* to believe

89. H.R. REP. No. 103-827, at 31 (1994), *reprinted in* 1994 U.S.S.C.A.N. 3489, 3511; *See also* Communications Assistance For Law Enforcement Act, § 207(a), Pub. L. No. 103-414, 108 Stat. 4279, 4292 (codified as amended at 18 U.S.C. § 2703(c) (1994)).

90. H.R. REP. No. 103-827, at 31 (1994), *reprinted in* 1994 U.S.S.C.A.N. at 3511.

91. *Id.*

92. 18 U.S.C. § 2703(a)(1)(B)(i)–(iii) (1994).

93. Communications Assistance for Law Enforcement Act, § 207(a)(2), Pub. L. No. 103-414, 108 Stat. 4279, 4292 (1994).

that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[94]

The intent behind the establishment of an intermediate standard was to protect on-line transactional records against, in the Judiciary Committee's words, " 'fishing expeditions' by law enforcement."[95]

On its face, § 2703 applies well to Carnivore "pen register" installations. An ambiguous legislative history, however, complicates such a conclusion. § 2703 is part of Chapter 121, entitled "Stored Wire and Electronic Communications and Transactional Records Access." As such, § 2703 would appear to apply only to "transactional logs" compiled by ISPs. Such logs consist of electronically stored records detailing the totality of a subscriber's online activities—to and from whom she sent and received e-mails, what web sites she viewed, what commercial transactions she completed, etc. Supporting this narrow construction is the House Judiciary Committee's expression of concern about law enforcement access to just such compilations of data.[96]

And yet there are plausible arguments that § 2703 applies to "real-time" collection of transactional data as well. First, Congress may have distinguished between the contents of communications and transactional information by its choice of statutory language. § 2703(a) sets out when a service provider may be required to disclose "the contents of an electronic communication, that is in electronic storage."[97] Likewise, § 2703(b)(2) describes situations in which providers of "remote computing services" must disclose an "electronic communication that is held or maintained on that service."[98] § 2703(c) and (d), however, do not so limit the transactional records (including e-mail addressing information) protected by the intermediate standard. Instead, these latter sections speak generally of instances when a provider of electronic communications must disclose "a record or other information pertaining to a subscriber to or customer of such service."[99] This difference in statutory language, as suggested by the court in *In re Cellular Telephone Digital Analyzer*,

94. 18 U.S.C. § 2703(d) (Supp. IV, 1998) (emphasis added).

95. H.R. REP. No. 103-827, *supra* note 89, at 31 (1994), *reprinted in* 1994 U.S.S.C.A.N. at 3511.

96. *Id.* at 17, *reprinted in* 1994 U.S.S.C.A.N. at 3497. ("Transactional records documenting these activities and associations are generated by service providers. For those who increasingly use these services, this transactional data reveals a great deal about their private lives, all of it compiled in one place.")

97. 18 U.S.C. § 2703(a) (1994).

98. 18 U.S.C. § 2703(b)(2) (1994).

99. 18 U.S.C. § 2703(c)(1)(B) (Supp IV 1998).

"cannot be assumed to be inadvertent."[100] It may well reflect Congress' wish to afford greater protection to transactional data (including e-mail addressing information) without regard for when it was acquired.

A much stronger ground for holding § 2703 applicable to real-time acquisition of e-mail addressing information is the questionable difference between "disclosure" of stored records and "interception" of transactional data. The committee's concern, as previously noted, was that law enforcement would gain access to entire transactional logs, from which they could effectively recreate a subscriber's online activities "without any judicial intervention."[101] CALEA therefore implemented the "intermediate standard" of § 2703(d) to increase judicial oversight of government access to such records.

A Carnivore installation enables the FBI to create just such a transactional log itself, with the scope determined only by the remotely controlled configuration of the system's filters. If authorized by a § 3123 pen register order, this record is created without any effective "judicial intervention"[102] in just the way Congress sought to prevent with CALEA. The data sets "disclosed" by an ISP and "intercepted" by Carnivore are identical but for the owner (and controller) of the equipment by which they are recorded. Thus, the only appreciable difference between acquiring e-mail addressing information through a § 2703 "disclosure" and a § 3123 pen register "interception" is that the latter allows the FBI more control with less oversight.

Allowing the FBI to construe § 2703 to permit such a result would contravene the policy of heightened protection for transactional records that Congress intended that section to serve. Principles of statutory construction dictate that the executive branch may not administer a statute in a manner inconsistent with the administrative structure Congress has enacted in law.[103] Thus, where the intent of Congress is clear (as it is with § 2703), both the courts and the agency are bound to give effect to that intent.[104] It follows that Carnivore pen register installations, in which "transactional records" in the form of e-mail addressing information are to be obtained, may only be authorized under the intermediate standard

---

100. *In re* Application of the U.S.A. for an Order Authorizing the Use of a Cellular Telephone Digital Analyzer, 885 F. Supp. 197, 200 (C.D. Cal. 1995).

101. H. R. REP. No. 103-827, *supra* note 89, at 19, *reprinted in* 1994 U.S.S.C.A.N. at 3497.

102. Recall that the court "shall enter" (18 U.S.C. § 3123(a) (1994)) a pen register order upon the requesting agent's certification that "the information likely to be obtained is relevant to an ongoing criminal investigation." (18 U.S.C. § 3122(b)(2) (1994)).

103. 2 AM. JUR. 2D *Administrative Law* § 525 (1994) (citing ETSI Pipeline Project v. Missouri, 484 U.S. 495, (1988)).

104. *Id.* (citing K-mart Corp. v. Cartier, Inc., 486 U.S. 281 (1988) *and* ETSI Pipeline Project v. Missouri, 484 U.S. 495 (1988).

of 18 U.S.C. § 2703. For courts to exempt such an activity from the scope of § 2703, and instead authorize it under § 3123, contravenes congressional intent with regard to § 2703.

One must immediately note the increased burden this places upon FBI agents seeking Carnivore pen register orders. The *ex parte* order issued for traditional pen registers, pursuant to which the FBI currently deploys Carnivore in pen mode, requires only the law enforcement official's certification that the "information likely to be obtained by such installation and use is relevant to an ongoing investigation."[105] Worded in the mandatory ("the court *shall* enter an ex parte order"),[106] this provision hamstrings the magistrate reviewing the order, as the Senate Judiciary Committee noted: "This provision does not envision an independent judicial review of whether the application meets the relevance standard, rather the court needs only review the completeness of the certification submitted."[107]

By contrast, a § 2703 order requires an actual statement of "specific and articulable facts."[108] Moreover, the reviewing magistrate must determine (i.e. independently review) that these facts establish "reasonable grounds" to believe the requested records are both "relevant and material" to an ongoing investigation.[109] Applied to a Carnivore installation in pen mode, as seems appropriate from the discussion *supra*, § 2703 significantly limits the circumstances in which the FBI can justify implementation of a Carnivore pen register.

4. Carnivore Does not Meet the Minimization Requirements of 18 U.S.C. § 3121

Even if pen register statutes could be stretched to include Carnivore installations, the program's current incarnation arguably violates the minimization requirement of 18 U.S.C. § 3121. That section, also added by CALEA section 207, states, "A government agency authorized to install and use a pen register under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing."

The version of Carnivore tested by the IITRI researchers records not only the "To:" and "From:" fields of e-mail messages, but also the length of all other fields, capturing the full-text of messages and replacing text

105. 18 U.S.C. § 3123(a) (1994).
106. *Id.* (emphasis added).
107. S. REP. No. 99-541, pt. 4, at 47 (1986), *reprinted in* 1986 U.S.S.C.A.N. at 3601.
108. 18 U.S.C. § 2703(d) (Supp. II 1996).
109. *Id.*

in all other fields with Xs.[110] Remembering also the IITRI team's suggestions for simple ways to eliminate collection of this additional information,[111] better technology is clearly "reasonably available" to limit the data Carnivore captures to what is ostensibly "dialing and signaling information." If for no other reason than this alone, the FBI should not be allowed to use the tested version of Carnivore as an Internet pen register.

PART IV. CONCLUSION

The above analysis demonstrates that current law requires that the FBI meet the "intermediate standard" (specific and articulable facts showing reasonable grounds for believing information sought is relevant and material) of 18 U.S.C. § 2703 to intercept e-mail addressing information using the Carnivore system. Despite its claim of authority under a conflation of the pen register standard of 18 U.S.C. § 3123 (mere certification that information is relevant to ongoing investigation) and the § 2703 standard,[112] the law dictates that federal courts not permit such interceptions under the more lenient § 3123 standard.

State and federal law enforcement officials are constitutionally permitted to intercept e-mail addressing information under *Smith*, *Miller*, and *Katz*. Because such information is voluntarily conveyed to and may be recorded by a third party—the sender's ISP—for legitimate business purposes, Internet users may not claim either a subjective or an objective expectation of privacy in that information. In this manner, the use patterns of e-mail addresses and telephone numbers by both consumers and service providers analogize well. The analogy is shattered by any collection of information in excess of the IP addresses and "To:" and "From:" fields of e-mail messages, however. Such collection violates the Fourth Amendment and must be eliminated from Carnivore's program to bring it within constitutional limits.

Assuming this constitutional flaw in the program is remedied,[113] Carnivore nevertheless fails to satisfy federal statutory requirements for a pen register order under the lenient standard of § 3123 for three reasons. First, Congress explicitly removed e-mail addressing information from the scope of § 3123 when it passed CALEA section 207, codified

110. ILLINOIS INSTITUTE OF TECHNOLOGY RESEARCH INSTITUTE, *supra* note 21, at xii, 4-2.

111. *Id.* at A-1.

112. *Senate Hearing*, *supra* note 10 (statement of Donald M. Kerr).

113. And if the FBI truly desires to stay within constitutional bounds, there is no reason why the problem shouldn't be fixed.

in 18 U.S.C. § 2703. Second, Carnivore does not meet the statutory definition of a pen register in 18 U.S.C. § 3127, because it is not "attached to a telephone line." Judicial interpretation of the pen register statute in relation to other new technologies, as well as indicia of congressional intent, support this conclusion. Finally, even if Carnivore could be considered analogous to a pen register under § 3127, the version tested by IITRI collects more information (field and message lengths) than permitted by a pen register order, violating the minimization requirement of 18 U.S.C. § 3121.

The requirements of § 2703 represent a reasonable standard for the authorization of Carnivore interceptions of e-mail addressing information. This standard balances the important competing social interests implicated in Carnivore installations. On the one hand, it lends a measure of protection to the privacy of Internet users by requiring federal law enforcement to come forward with specific facts that prove the necessity of and justification for using such an intrusive technology, rather than granting them access via the "rubber-stamp" standard of § 3123. On the other hand, the standard does not erect such a high barrier to Carnivore installations that law enforcement is prevented from using this indisputably effective technology to investigate very real and very serious crimes. In the absence of further legislative direction, the § 2703 standard should be applied as the most legally and politically defensible interpretation of existing law.

PART V. EPILOGUE: THE USA PATRIOT ACT

A. *Introduction*

On October 26, 2001, Congress enacted Public Law 107-56, the acronym-conscious Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 [hereinafter Patriot Act]. Pushed quickly through Congress in response to the attacks of September 11, 2001, the Patriot Act expanded the powers of law enforcement in an effort to combat terrorist acts domestically and worldwide.[114] Section 216 modifies the restrictions on pen register and trap and trace installations.[115] The provisions of section 216 work a radical change in the law of pen registers, for

114. *See* USA PATRIOT Act, Pub.L. 107-56, 115 Stat. 272 (Oct. 26, 2001) [hereinafter "Patriot Act"] ("An Act to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes.").

115. *See id.* § 216, 115 Stat. 272, 288–90.

the first time explicitly expanding the scope of 18 U.S.C. §§ 3121–3127 (1994) to authorize pen register installations in the Internet context.[116]

With the government's efforts currently focused on combating terrorism, sections of the Patriot Act affecting the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1842) [hereinafter FISA] are also likely to play an important role in the use of Internet pen registers. Section 214 of the Patriot Act alters the language of FISA section 402 to broaden the range of investigations in which pen registers may be employed to combat terrorism.[117] Section 214 permits the use of pen registers to monitor a United States person only so long as the investigation "is not conducted solely upon the basis of activities protected by the first amendment to the Constitution."[118]

The net effect of the changes wrought by sections 214 and 216 is to statutorily legitimate and expand government monitoring of Internet traffic in the same manner as telephone communications. The Patriot Act resolves most lingering statutory questions as to whether a tool like Carnivore may be employed as an Internet pen register by expressly including such applications in the relevant definitions and procedures. One may still question, however, whether Carnivore pen register installations meet constitutional and minimization requirements if the device continues to go beyond collecting "dialing, routing, addressing, and signaling information"[119] to also collect the X-redacted contents of e-mail messages.[120] This Epilogue briefly explains the effects of Patriot Act sections 214 and 216, and considers their implications for the legality of Internet pen registers.

B. *The New Face of Pen Register Law*

1. Carnivore Moves Permanently onto the Internet: Patriot Act Section 216

The provisions of section 216 most radically altered the existing law of pen registers, and merit the most thorough examination. Section 216 not only redefined many key terms that explicitly expand the statute's scope to include Internet pen registers, but also imposed record-keeping

116. *See, e.g., id.* § 216(b), 115 Stat. at 288–90 (including in new 18 U.S.C. § 3123(a)(3)(A) specific requirements in relation to pen registers installed on packet-switched networks).

117. *See id.* § 214, 115 Stat. at 286–87 (permitting pen registers for "any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities").

118. *Id.* § 214(a)(1), 115 Stat. at 286.

119. 18 U.S.C. § 3121(c) (2001), *amended by* Patriot Act § 216(a)(2), 115 Stat. at 288.

120. *See supra* Part IV.A.2.

requirements that create an "electronic paper trail" permitting after-the-fact judicial oversight of the installation. Moreover, section 216 permits law enforcement officials to cast a broad net by permitting the court order to be served on any communications service provider whose assistance is necessary to facilitate execution of the order.

As discussed in Parts IV.B.1–2, pen register law was previously ill suited to accommodate Carnivore installations because its definitions were cast in terms of telephone facilities and functions.[121] Courts were largely unwilling to stretch those definitions to allow pen registers to be utilized with non-telephone technologies.[122] As such, the statutory authorization for Internet applications of Carnivore in pen register mode was highly questionable.

Patriot Act section 216 lays those questions to rest by systematically redefining pen registers in terms that encompass Internet applications. Pen registers and trap and trace devices themselves now include any "device *or process*" that captures, records or decodes "dialing, *routing, addressing, or signaling* information,"[123] rather than simply "the numbers dialed" or "the originating number."[124] Pen registers now reach not only information "transmitted on the telephone line to which such device is attached,"[125] but rather any of the specified information "transmitted by an instrument or facility from which a wire or electronic communication is transmitted."[126] Congress also eliminated the telephone limitation by inserting "or other facility" after references to "the telephone line."[127] Section 216 seems to explicitly incorporate the pen register limitation suggested by the *Smith* Court[128] by adding to the very definition of pen register and trap and trace devices the qualification "provided, however, that such information shall not include the contents of any communication."[129]

---

121. *See, e.g.*, 18 U.S.C. § 3127(3) (1994) (amended 2001).

122. *See, e.g.*, Brown v. Waddell, 50 F.3d 285, 290–91 (4th Cir. 1995); *In re* Application of the U.S.A. for an Order Authorizing the Use of a Cellular Telephone Digital Analyzer, 885 F. Supp. 197 (C.D. Cal. 1995).

123. Patriot Act § 216(c)(2)–(3), 115 Stat. at 290 [emphasis added].

124. 18 U.S.C. §§ 3127(3)–(4) (1994) (amended 2001).

125. 18 U.S.C. § 3127(3) (1994) (amended 2001).

126. 18 U.S.C. § 3127(3) (2001), *amended by* Patriot Act § 216(c)(2)(A), 115 Stat. at 289. Trap and trace devices were defined to apply to wire or electronic communications. *See* 18 U.S.C. § 3127(4) (1994) (amended 2001).

127. *See* Patriot Act §§ 216(b)(2)(A)–(B), (b)(3)(A), (c)(6), 115 Stat. at 289–90.

128. *See supra* Part IV.A.2. (emphasizing importance to *Smith* decision of fact that pen registers disclose only the telephone numbers that have been dialed and not the purport of communications, the identities of the parties, or whether the call was even completed).

129. 18 U.S.C. § 3127(3)–(4) (2001), *amended by* Patriot Act § 216(c)(2)–(3), 115 Stat. at 290.

These amendments merely bring the statutory language into line with actual modern practice, in which Carnivore has been employed by the FBI as an Internet pen register on numerous occasions. Perhaps more important from the standpoint of fighting terrorism, section 216 went on to ease law enforcement's burden when obtaining and utilizing Carnivore orders in two significant ways. First, Congress made pen register orders (for any medium) issued by federal District Courts applicable "anywhere within the United States."[130] Previously, federal courts were only authorized to issue orders applicable within their district.[131] Second, and more radically from the perspective of Internet Service Providers, section 216(b)(1) makes pen register orders applicable "to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order." In other words, law enforcement personnel need not designate in advance on which ISP's network they will install a Carnivore pen register–any are subject to the order if a copy is served on them. If the ISP is not named in the order, all the law enforcement official must do is "provide written or electronic certification that the order applies to the person or entity being served."[132]

The truly revolutionary aspect of section 216 is found in its record-keeping requirements for pen registers attached to packet-switched networks (like the Internet). Section 216(3)(A) requires law enforcement agencies installing and using their own pen register or trap and trace devices on a packet-switched data network of a public communication service provider to ensure that a record is maintained which identifies:

(i) any officer or officers who installed the device and any officer or officers who accessed the device to obtain information from the network;

(ii) the date and time the device was installed, the date and time the device was uninstalled, and the date, time, and duration of each time the device is accessed to obtain information;

(iii) the configuration of the device at the time of its installation and any subsequent modification thereof; and

(iv) any information which has been collected by the device.

To the extent that the pen register or trap and trace device can be set automatically to record this information electronically, the record shall be maintained electronically throughout the installation and use of such

130. Patriot Act § 216(b)(1), 115 Stat. at 288.
131. 18 U.S.C. § 3123(a) (1994) (amended 2001).
132. Patriot Act § 216(a)(1), 115 Stat. at 288.

device.[133] Within 30 days of the expiration of the pen register order, this audit record must be provided ex parte and under seal to the authorizing court.[134]

The Carnivore version reviewed by IITRI (Carnivore 1.3.4) did not possess the ability to automatically record the required information. The IITRI report states that it is impossible to determine which individual agent set or changed filter settings; that the relationship between filter settings, collected data, and other investigative activities may be difficult to establish; that it is not possible to definitively show what settings were used to collect any given set of data; and that the time and date stamps placed on data are subject to error.[135] In its then-current incarnation, Carnivore provided nothing in the way of security or accountability. As the IITRI report put it, "since there are no checksums or other protections on the collected data files and no individual accountability, anyone could edit the collected data. Since all users log on as Administrator, evidence of the changed files could be erased."[136] In light of these revelations, and without any public review of subsequent Carnivore versions, one may well question just how much control section 216's audit requirements will give courts over the use of Internet pen registers.

What the Patriot Act does not change is the low evidentiary standard law enforcement officials must satisfy to obligate the court to issue pen register orders. Upon an application setting out 1) the identities of the government agent making the application and the law enforcement agency conducting the investigation, and 2) a certification by the applicant that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation, the court is required to issue an *ex parte* order authorizing the pen register or trap and trace installation.[137] The only difference is that now the court may issue an order based on this scant evidentiary basis—that applies anywhere within the United States.[138]

On the whole, section 216 solidifies the place of Internet pen registers in American criminal investigations. Bringing the statutes definitionally in line with existing practice, it eliminates questions of Congressional intent and statutory interpretation with regard to different communications technologies. In order to aid in the "war on terrorism,"

133. *Id.* § 216(c)(3)(A), 115 Stat. at 290.

134. *Id.* § 216(c)(3)(B), 115 Stat. at 290.

135. ILLINOIS INSTITUTE OF TECHNOLOGY RESEARCH INSTITUTE, *supra* note 21, at 4-4 to 4-5.

136. *Id.* at 4–5.

137. *See* 18 U.S.C. § 3123(a) (2001), *amended by* Patriot Act § 216(b)(1), 115 Stat. at 288.

138. *Id.*

the statute further streamlines the process of applying for and executing a pen register order, allowing any federal court to issue an order applicable anywhere in the country to any communications provider whose assistance is required. Moreover, the changes brought about by section 216 are permanent. Most of the provisions of Patriot Act Title II are subject to a "sunset provision" causing them to expire on December 31, 2005.[139] Section 216, however, is expressly exempted from the sunset provision, meaning the changes it makes to pen register authorities are here to stay.[140]

2. The War on Terrorism's Secret Weapon: Patriot Act Section 214

The Foreign Intelligence Surveillance Act (FISA) controls the use of electronic surveillance techniques to gather foreign intelligence information within the United States. Patriot Act § 214(a) makes an important change to the scope of FISA's pen register and trap and trace provisions, found in 50 U.S.C. § 1842. In defining the purposes for which a pen register may issue under FISA, Patriot Act § 214(a)(1) replaces "for any investigation to gather foreign intelligence information or information concerning international terrorism"[141] with:

> for any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.[142]

The most important aspect of this new language is the phrase "to protect against international terrorism." In the wake of September 11, 2001, these words carry a broad mandate to monitor the destinations and origins of communications sent and received by individuals or organizations thought to have some connection with international terrorism. Even before the criminal investigation necessary to obtain a pen register order commences (or indeed, even if one never materializes), government officials may investigate individuals suspected to be linked in any way to terrorism.

Prior to passage of the Patriot Act, the applicant for a FISA pen register was required to provide information demonstrating there was reason for believing that the communications device to which the pen register

139. Patriot Act § 224(a), 115 Stat. at 295.
140. *Id.*
141. 50 U.S.C. § 1842(a)(1) (Supp. 1999) (amended 2001).
142. Patriot Act § 214(a)(1), 115 Stat. at 286.

would be attached had been or was about to be used to facilitate terrorist activities.[143] Patriot Act § 214(a)(3) eliminates this requirement, reducing the burden on officials wishing to employ an anti-terrorism pen register to that required for ECPA pen registers—an application giving the identity of the officer seeking to use the pen register and a certification that the information likely to be obtained is relevant to the relevant type of investigation.[144]

FISA will play a prominent role in the ongoing war against terrorism. Even more than the ECPA amendments, the changes to FISA authorize broad use of pen registers and trap and trace devices. Where criminal charges are not pending or even contemplated, FISA will serve as the government's primary means of collecting information on suspected terrorist collaborators within the United States. The changes to FISA, however, are subject to the Patriot Act's sunset provision.[145] Foreign intelligence investigations commencing before December 31, 2005, are an exception, and will continue under the amended FISA provisions.[146]

C. *Implications of USA PATRIOT Act for Previous Analysis*

The USA PATRIOT Act represents a quantum leap forward in bringing the law of pen registers in line with contemporary practice on the Internet. The reality of ubiquitous online communications could not long exist without law enforcement seeking and securing investigatory powers on the network. Indeed, they have already been exercising such powers since at least June 2000, when Carnivore's existence was revealed to the public. Congressional action was necessary to demarcate the extent of those powers and to place appropriate controls on their exercise.

To that end, Congress updated the relevant statutory definitions to include Internet pen registers within pen registers generally. This in itself was not terribly revolutionary; courts issuing Carnivore pen register orders had already assumed the statutes extended to the Internet. Congress simply approved this assumption. As such, the criticisms of Parts IV.B.1.–3. are now moot. The literal language of 18 U.S.C. §§ 3123 and 3127 have been altered to allow Carnivore pen register installations. Any judicial interpretations suggesting the contrary based on the statute's limitation to a telephone line are likewise superceded. While the argument in Part IV.B.3. that CALEA evidenced a congressional intent to

143. 50 U.S.C. § 1842(c)(3) (Supp. 1999) (amended 2001).
144. Patriot Act § 214(a)(3), 115 Stat. at 286.
145. *Id.* § 224(a), 115 Stat. at 295.
146. *Id.*

impose a higher standard of proof for obtaining e-mail addressing information can no longer stand, there remains some inconsistency in requiring law enforcement to meet a higher standard for obtaining transactional logs directly from the service provider than for creating such logs themselves.

The record keeping requirements of Patriot Act § 216(b)(3)(A) are an encouraging sign that Congress expects courts to exercise some oversight of Internet pen register use. Assuming the absence of overt alterations of the audit record, courts should use these records to insure that the scope of the pen register order is not exceeded. As noted above, however, technical limitations in the Carnivore program may render such oversight illusory. The only publicly reviewed version of the software allowed the wholesale alteration of data without producing evidence of such alteration. One may well question whether law enforcement will implement more conscientious record-keeping in a time of increased public receptiveness to invasive monitoring techniques.

Despite the sweeping changes introduced by the Patriot Act, the troubling question remains whether Carnivore collects more than is constitutionally permissible for a pen register.[147] The capture of X-redacted subject and content information appears to violate the *Smith* Court's requirement that pen registers collect only information in which no expectation of privacy exists (in that case, the telephone numbers dialed). While not revealing what those contents are, the additional information does disclose whether a communication was completed.[148] Likewise, this over-collection appears to violate the minimization requirement of 18 U.S.C. § 3121(c). As amended, it reads:

> (c) Limitation. A government agency authorized to install and use a pen register or trap and trace device under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications.

The IITRI suggested ways in which this minimization requirement could be met, and opined that the then-current version of Carnivore may have failed to meet those requirements.[149] With no subsequent report to indicate whether these recommendations were followed, it is currently

147. *See supra* Part IV.A.2.

148. *See* Smith v. Maryland, 442 U.S. 735, 741 (1979).

149. *See* ILLINOIS INSTITUTE OF TECHNOLOGY RESEARCH INSTITUTE, *supra* note 21, at xii, A-1.

unknown whether Carnivore or its successors are collecting data within constitutional and statutory boundaries. The audit records provided to courts will shed no light on this question for the public, for even assuming they are accurate, they are kept under seal by the court.

The changes implemented by Patriot Act sections 214 and 216 will likely increase the number of pen register and trap and trace orders issued for Internet communications. Section 216 permanently authorizes Internet pen registers for criminal investigations. Section 214 temporarily but sweepingly expands the permissible reasons for installing an Internet pen register. In tandem, they open the Internet to police surveillance and shatter any illusions that online communications are privileged in any manner greater than more traditional telecommunications media.